IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application Of : Atty Dkt#: PKAY-P1

KATSIKAS

: Examiner: Hoffman, Brandon S.

Serial No.: 09/648,894

: Group No: 2136

Filing Date: August 25, 2000

Title: SYSTEM FOR ELIMINATING UNAUTHORIZED ELECTRONIC MAIL

AFFIDAVIT OF KATSIKAS UNDER 37 C.F.R. 1.132

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

The undersigned, PETER KATSIKAS, declares as follows:

1. I was CEO and Owner for 10 years of CyberCom, Inc., a system integration and Web development firm based in Honolulu, HI. Prior to that, I was employed by XenTec Software Engineering for 6 years, working on computer and network systems. I am certified as an authorized Technical Service Representative by Microsoft, since 1997. Throughout 22 years of my career in this field, I have designed, installed, and maintained computer systems and network systems of all types for companies, institutions, and government agencies throughout the entire range of enterprise applications. I am also the inventor in the present U.S. patent application. I submit this Affidavit in support of the patentability of the claims as amended in the current Response to the Office Action in this case.

Patent Application Claims

2. The invention sought to be patented is defined in main Claims 21, 32, and 40 which are amended concurrently herewith to read as follows:

21. A method for eliminating unauthorized email on a network comprising the steps of:

(a) establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) of email addresses of [~~external users~~] senders authorized to send email to the user,

(c) receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address;

(d) causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list; and

(e) if the sender address of the intended email is recognized as being on the user's ASL list, causing the email-receiving server under the common email-sending system protocol to send a reply message to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is not recognized as being on the user's ASL list, causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server [~~that the email-receiving server will not accept the sending of the email to the email-receiving server~~] so as to prohibit the email-sending server from sending the intended email to the email-receiving server, whereby the sender is unable to send the unwanted email to the user and is deterred from sending further email to the user's address indicated to be in error by the email-receiving server.

32. A method for eliminating unauthorized email on a network comprising the steps of:

(a) establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) which identifies email addresses of senders not authorized to send email to the user;

(c) receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address;

(d) causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list of [~~external users~~] senders not authorized to send email to the user; and

(e) if the sender address of the intended email is recognized as being on the user's ASL list, causing the email-receiving server under the common email-sending system protocol to send a reply message to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is recognized as being not authorized on the user's ASL list, causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server [~~that the email-receiving server will not accept the sending of the email to the email-receiving server~~] so as to prohibit the email-sending server from sending the intended email to the email-receiving server, whereby the sender is unable to send the unwanted email and is deterred from sending further email to the user's address indicated to be in error by the email-receiving server.

40. A system for eliminating unauthorized email on a network comprising:

(a) first means for establishing a connection on a network between an email-receiving server and an email-sending server, wherein said email-receiving server and email-sending server utilize a common email-sending system protocol to send email on the network;

(b) second means for making accessible to the email-receiving server for each subscribing user an authorized senders list (ASL list) for identifying which email addresses of [~~external users~~] senders are authorized to send email to the user;

(c) third means for receiving at the email-receiving server, under the common email-sending system protocol, a message from the email-sending server requesting to send email which is addressed to a user deemed to receive email through the email-receiving server and which is addressed from a given sender address; and

(d) fourth means for causing the email-receiving server to check whether the user the intended email is addressed to is a user which receives email through the email-receiving server, and, if so, then causing the email-receiving server to check whether the sender address of the intended email is on the user's ASL list as being authorized to send email to the user;

(e) wherein, if the sender address of the intended email is recognized as being authorized on the user's ASL list, said fourth means causing the email-receiving server to send a reply message, under the common email-sending system protocol, to the email-sending server that the sending of the email to the email-receiving server will be accepted, otherwise if the sender address of the intended email is not authorized on the user's ASL list, said fourth means causing the email-receiving server to send an error message, under the common email-sending system protocol, to the email-sending server [~~that the email-receiving server will not accept the sending of the email to the email-receiving server~~] so as to prohibit the email-sending server from sending the intended email to the email-receiving server, whereby the is unable to send the unwanted email and is deterred from sending further email to the user's address indicated to be in error by the email-receiving server.

Difference of the Claimed Subject Matter Over the Cited Prior Art

3. In the present Office Action, the Examiner rejected Claims 21-23, 28-34, and 37-40 as unpatentable for obviousness over Hashimoto U.S. Patent 5,931,905, in view of Paul U.S. Patent 6,052,709, and Claims 24-27, 35-36 further in view of Lillibridge U.S. Patent 6,195,698. The Claims as presented and the Applicant's argument clearly stated that the unique feature of the claimed invention is that the standard email-sending protocol is utilized to enable the email-receiving server to reject unauthorized email from a sender who is not on the user's Authorized Senders List (ASL). The Examiner cited the Paul patent as teaching that spam probes can be used to generate a list of suspected addresses of spammers sending spam email, and a standard email-sending protocol (such as MAPI) can be used to identify email sent by a suspected spammer and cause the email-receiving server to delete it.

4. Therefore, main Claims 21, 32, and 40 have been amended to specifically recite that if the sender address of the intended email is not recognized as an authorized sender on the user's ASL list, the email-receiving server sends an error message, under the common email-sending system protocol, to the email-sending server indicating that email addressed to the user will not be accepted at the email-receiving server so as to prohibit sending the intended email to the user, whereby the sender is unable to send the unwanted email and is deterred from sending further email to the user's address indicated to be in error by the email-receiving server.

5. The function in the present invention of sending an error message indicating that email addressed to the user will not be accepted and causing the email to be blocked from being sent in the first place, and deterring the spammer from further sending email to the user's address, is a distinctly different approach and provides an important advantage not recognized in the Hashimoto and Paul patents. Both cited references repeatedly state that the email is first received, then if it is recognized as being from an unwanted sender, it is eliminated before being placed in the user's mailbox (Hashimoto) or from being stored on the receiving server (Paul). In contrast, the amended claims define the result in the present invention that the

email is blocked before it can be sent by the sending server and the spammer is deterred from further spamming to that user by receiving the error message indicating that email addressed to that user address will not be accepted.

Evidence of Non-Obviousness

6. I believe that the function of selectively blocking email from a sender not on the user's ASL list before it can be sent and also deterring the spammer from further spamming by sending an error message under the common email-sending protocol was not recognized in the industry prior to my invention. The computer industry has long sought a capable solution to the burgeoning spam problem. At the time of my invention, the state of the art in the industry was based on analyzing the header addresses and/or contents of email in order to filter out spam, which absolutely requires that the email first be received. Both Hashimoto's and Paul's teachings are squarely based on receiving the email first and then comparing the email content against its exclusion databases and rules to determine further actions. Neither of them teaches the radical modification of the receive process to reject receipt of the email in the first place by sending an error message indicating that email addressed to the user will not be accepted. The significant advantage of my invention is that by blocking the email from being sent, the user enjoys a truly spam-free experience, and the spammer is immediately deterred from further spamming to that user.

7. Perhaps the best proof that the filtering paradigm has been unsuccessful is the fact that today we have more spam than ever before. A recognized industry watchdog CAUCE lists filtering as a "non-solution", http://www.cauce.org/about/nonsolutions.shtml. To the best of my knowledge, there has been no published information that teaches my invention as described in the present Specification and specifically shown in Fig. 7b. I believe that my approach of blocking email from being sent with an error message when not authorized on a user's ASL list and deterring further spamming is a vast improvement on the state of the art. Other technologies have always either applied filtering rules after the email has been received, as

in the case of both Paul and Hashimoto, or applied exclusion rules universally as to all recipients on a given server from receiving email from a blacklisted sender. None of the prior approaches have taught or suggested my selective exclusion technique of using the common email-sending protocol when a sender address is not authorized on a user's ASL list to send an error message telling the sending server that the email will not be accepted. The fact that my approach has still been not published by anyone else four years after the filing of my patent application is further evidence of the non-obviousness of this invention.

8. My email blocking, error-message sending system has been installed and tested with several ISPs in the U.S., and has been praised for the unique results it achieves. These ISP customers have recognized that my selective exclusion technique using the common email-sending protocol is a new approach that is qualitatively different than other approaches, as evidenced in the letters of endorsement as users of the product appended hereto. (3 letters)

9. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

AFFIANT: PETER KATSIKAS

Dated: August 9, 2004

At: Honolulu, HI

Internet and Telecommunication Services

100-A Twinbridge Drive, Pennsauken, NJ 08110 • 1-888-SNIP-600 • Fax: 856-662-8641 • www.snip.net • sales@snip.net

August 6, 2004

To whom it may concern:

As an Internet Service Provider, SNiP Internet and Telecommunications, Inc. has observed the steady increase in SPAM or junk mail volume over the last seven years. Currently, 60 to 80 percent of ***all*** mail we process falls into the category of unsolicited commercial e-mail or SPAM. We have tried many different approaches towards stemming the tide of junk mail including custom designed filters and blacklists, global public blacklists, and traditional SPAM filtering based on e-mail message content. While we experienced some degree of success using those approaches, our customers were still receiving unacceptable levels of SPAM. In addition, a significant portion of company infrastructure and man-hours had to be devoted to the fight to reduce the flow of SPAM into our user's mailboxes.

The core problem with the methods we used, as well as all other spam solutions we examined, is that they are reactive in nature and require that we devote company hardware and man-hours to analyze SPAM ***after it has been received.*** The fact that we had to accept the mail, before determining whether or not it was SPAM, required significant infrastructure, bandwidth, and labor. Spammers do not sit still. They are continually moving from network to network, registering new domain names, and altering the format of their messages to get around conventional filtering systems.

In March of 2004 we began using a new anti-spam technology from Titan Key, a Hawaii company headed by Peter Kay. We have found that Titan Key is the only product in the marketplace that allows each and every mail user to control exactly what mail enters their inbox via Titan Key's novel use of a "550 no such user" error message. The Titan Key system's use of the "550 no such user" error message at the earliest possible stage of the email transaction prevents SPAM from being sent ***at all.*** All the SPAM messages are left sitting on the Spammer's own server instead on SNiP's servers. The benefit for SNiP is that our bandwidth and server capacity no longer being hijacked by the Spammers because the email is never transferred from the Spammer's server to our mail servers. The benefit for the end user is that they never see unwanted mail and there is no cumbersome quarantine folder to check and maintain.

Our end users have found the product valuable and a significant improvement over previous products that any of us have tried. We will continue to use Titan Key's anti-spam technology. There is nothing else like it out there.

Sincerely,

Joseph J. Giacomelli
VP Customer Operations
SNiP Internet & Telecommunications, Inc

Pacific Information Exchange, Inc.
1132 Bishop Street, Suite 770
Honolulu Hawaii 96813

August, 4, 2004

To whom it may concern:

As an ISP (Internet Service Provider), Pacific Information Exchange, Inc. (PIXI.net) has found the spam problem to be particularly acute in our industry. ISPs are the victims of many spam attacks. We use different anti-spam approaches including blacklisting and traditional outsourced spam filtering based on email content and none of these approaches have delivered a satisfactory solution to the problem – our customers are still complaining about getting unacceptable levels of spam.

The problem with most spam solutions is that they are reactive and attempt to analyze spam after it has been received. This requires significant infrastructure, bandwidth, and continual maintenance due to the one-upmanship nature of the solution (much like anti-virus technologies).

In May of 2004 we began using a new anti-spam technology from Titan Key, a Hawaii company headed by Peter Kay. We have found Titan Key the only product in the marketplace that allows the end-user to control email flow to their inbox via a novel use of a "550 no such user" error message that is invoked at the earliest possible stage of the email transaction. This approach prohibits spam from entering our system. The benefit for us is that our bandwidth is not wasted because the email is never received in the first place. The benefit for the end user is that they never even see unwanted mail.

Our end users have found the product valuable and a significant improvement over previous products that either they or we have tried. Our users now have control over their email boxes. We plan on continuing to use Titan Key's anti-spam technology.

Sincerely,

Stan Kubota

Stan Kubota, President
Pacific Information Exchange, Inc

Painter & Green, LLC
218 Kaiko Isle Circle
Honolulu, HI 96825
Telephone 808 566 6618
Fax 808 566 6727

5 August, 2004

To whom it may concern,

Over the past few years, I have noticed the amount of spam sent to my inbox grow from a minor nuisance of 2-5 per day to an average of 200 unsolicited emails per day.

We have tried anti-spam software that included filtering, then challenge/response. This always reduced the problem, but it never truly solved it because all of these systems either swept the problem under the rug, or created a barrier that didn't allow legitimate mail to get through (Airline confirmations as an example).

Plus, sooner or later, spammers would find a way around the technology and once again our Inboxes started piling up with spam. (In the end, most of the spam we received appeared to come from people in our own net.)

Finally, even when the products were working properly, we still had to review a "spam folder" that contained suspected spam (or suspect addresses). Inevitably, this folder contained legitimate email that we had to recover and illegitimate e-mail that we had to open to find out that is was an ad for breast enhancement or penis enlargement.

In June of 2004, we began using a new anti-spam technology from Titan Key, a Hawaii company headed by Peter Kay. The results have been dramatic.

The weekend before the installation, my wife and I received 630 spam. 630. Since Titan Key was enabled, we haven't received a single spam. Not one. I cannot tell you what this means for our productivity.

And 'no spam' means that we have not had to review any spam folders because Titan Key's unique use of "550 no such user" error message prevents unwanted email from ever reaching our Inbox.

Overnight, our spam problem went away. Completely.

Titan Key also gives us the option of creating 'keymail' addresses that allows us to give an address to United Airlines that can only be used by United Airlines... nobody else can use it, so our mailbox is no longer a commodity to be bought and sold.

We enjoy a spam-free email experience. Titan Key is significantly better than anything else we have tried.

Sincerely,

Charles L. Painter
President

CP/lg